Notice of Allowability	Application No.	Applicant(s)	
	10/676,138	PATHAKIS ET AL.	
	Examiner	Art Unit	
	FARID HOMAYOUNMEHR	2439	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *response filed 2/11/2010*.

2. ☒ The allowed claim(s) is/are *1-20, 23 and 24, now re-numbered as claims 1-22*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *20100409* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

/Farid Homayounmehr/
Examiner
Art Unit: 2439

DETAILED ACTION

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Mr. Joe Mahrle on 4/7/2010.

The application has been amended as follows:

1. (Amended) A method for generating temporarily assigned identity information implemented in a computer-readable medium and executed on a proxy service to perform the method, comprising:

authenticating, by a proxy server, identity information associated with a request received from a requestor for accessing a service, the request is sent from the requestor to the service and intercepted for processing;

generating, by a proxy server, temporarily assigned identity information for the requestor, the temporarily assigned identity information is in a syntax and format recognized by the service,

and the temporary assigned identity information is unique to each of the requests and expires when the requestor terminates communication sessions associated with the services, and the temporarily assigned identity information includes a combination of, a password, a certificate, a token, a biometric value, a

hardware value, a network connection value, and a time value, and the temporarily assigned identity information is used to impersonate the requestors,

and the original identity information consists of a first subset, which reflects only those portions of the original identity information needed by the services to process the requests, and a second subset, which reflects all the information in the original identity information excluding the first subset,

and the temporary assigned identity information includes the first subset of original identity information for the requestors, and excludes the second subset,

~~and the temporary assigned identity information includes a subset of the identity information, the subset reflects only those portions of the identity information needed by the service to process the request;~~

updating, by a proxy server, a protected identity directory with the temporarily assigned identity information; and

directly transmitting, by a proxy server, the request and the temporarily assigned identity information to the service on behalf of the requestor, the service accesses the protected identity directory with the temporarily assigned identity information to authenticate the requestor for access, ~~and the temporarily assigned identity information is in a syntax and semantic format recognized and expected by the service for authenticating access to the service, and the service detects and denies multiple login events that use the temporary assigned identity information.~~

and the temporarily assigned identity information is monitored and removed from the protected identity directory and the local identity mapping store when terminating events are detected, and the proxy server detects and denies multiple login events that use the temporary assigned identity information.

2. (Amended) The method of claim 1 further comprising:

generating, by a proxy server, a mapping between the identity information and the temporarily assigned identity information; and

storing, by a proxy server, the mapping in a local identity mapping store.

3. (Amended) The method of claim 2 further comprising, synchronizing, by a proxy server, the local identity mapping store and the mapping with one or more addition local identity mapping stores.

4. (Original) The method of claim 1 wherein the generating further includes assembling an aggregate identity configuration for the requestor from one or more authoritative identity stores before generating the temporarily assigned identity information.

5. (Amended) The method of claim 1 further comprising, removing, by a proxy server, the temporarily assigned identity information from the protected identity directory after detecting a terminating event that terminates the authenticity of the temporarily assigned identity information.

6. (Amended) The method of claim 5 further comprising recycling, by a proxy server, a storage space occupied by the temporarily assigned identity information for use in a subsequent iteration of the method.

7. (Amended) The method of claim 1 further comprising:

detecting, by a proxy server, dynamic changes made on at least a portion of the identity information, wherein the changes are detected within the protected identity directory; and

synchronizing, by a proxy server, the temporarily assigned identity information with the changes.

8. (Amended) The method of claim 1 further comprising:

detecting, by a proxy server, dynamic changes made on at least a portion of the identity information, wherein the changes are detected within the protected identity directory; and

synchronizing, by a proxy server, the changes with one or more authoritative identity stores impacted by the changes.

9. (Amended) The method of claim 1 further comprising:

detecting, by a proxy server, changes made on at least a portion of the identity information, wherein the changes are detected within the protected identity directory; and

logging, by a proxy server, the changes for subsequent update with one or more authoritative identity stores impacted by the changes.

10. (Amended) A method for generating temporarily assigned identity information implemented in a computer-readable medium and executed on a proxy service to perform the method, comprising:

acquiring, by a proxy server, a request for a service from a requestor that makes the request directly to the service;

authenticating, by a proxy server, the request;

compiling, by a proxy server, an identity configuration for the request;

generating, by a proxy server, temporarily assigned identity information for the request using the identity configuration, and wherein the temporarily assigned identity information impersonates a requestor, and
the temporary assigned identity information is unique to each of the requests and expires when the requestor terminates communication sessions associated with the services, and the temporarily assigned identity information includes a combination of, a password, a certificate, a token, a biometric value, a hardware value, a network connection value, and a time value,

and the original identity information consists of a first subset, which reflects only those portions of the original identity information needed by the

services to process the requests, and a second subset, which reflects all the information in the original identity information excluding the first subset,

and the temporary assigned identity information includes the first subset of original identity information for the requestors, and excludes the second subset,

updating, by a proxy server, a protected identity directory with the temporarily assigned identity information; and

~~and the temporary assigned identity information includes a subset of original identity information for the requestor, the subset reflects only those portions of the original identity information needed by the service to process the request; and~~

directly transmitting, by a proxy server, the temporarily assigned identity information and the request to the service on behalf of the requestor, wherein ~~the temporarily assigned identity information is in a syntax and semantic format recognized by the service for authenticating the requestor for access to the service, and the temporary assigned identity information is unique to the request and expires when the requestor terminates a communication session associated with the service, and~~ a mapping between the identity configuration and the temporary assigned identity information is removed from cache when the request expires~~.~~

,and the proxy server detects and denies multiple login events that use the temporary assigned identity information.

11. (Previously Presented) The method of claim 10 wherein acquiring further includes, transmitting the request, wherein the request originates from a requestor's service over an insecure network.

12. (Original) The method of claim 10 wherein the transmitting further includes, transmitting the temporarily assigned identity information and the request to the service within a secure network.

13. (Amended) The method of claim 10 further comprising accessing, by the service on the proxy server, a protected identity directory to authenticate the request using the temporarily assigned identity information.

14. (Amended) The method of claim 10 further comprising:

acquiring, by a proxy server, an additional request issued from a same-requestor that is associated with the request, wherein the additional request is for an additional service;

authenticating, by a proxy server, the additional request; and

transmitting, by a proxy server, the temporarily assigned identity information and the additional request to the additional service.

15. (Amended) The method of claim 10 further comprising, forcing, by a proxy server, the temporarily assigned identity information to expire upon detection of a terminating event.

16. (Previously Presented) The method of claim 10 wherein the compiling further includes aggregating identity policies from one or more authoritative identity stores, wherein the identity policies are associated with the requestor that issued the request for the service.

17. (Amended) An identity information management system, comprising:

a proxy server that intercepts requests made for services, the requests are associated with requestors, and the requests are made from the requestors directly to the services and are processed by the proxy server;

a local identity mapping store for housing mappings between temporarily assigned identity information and identity configurations, the temporarily assigned identity information and the identity configurations are generated from identity information provided with the requests; and

a protected identity directory updated with the temporarily assigned identity information and accessed by the services in order to authenticate the requests, the requests and the temporarily assigned identity information are directly transmitted to the services on behalf of the requestors by the proxy server and the temporarily assigned identity information is in a syntax and semantic format recognized by the services for authenticating access to the services, and the temporary assigned identity information is unique to each of the requests and expires when the requestor terminates communication sessions associated with the services, and the temporarily assigned identity information includes a combination of, a password, a certificate, a token, a biometric value, a hardware value, a network connection value, and a time value, and the temporarily assigned identity information is used to impersonate the requestors,

and the original identity information consists of a first subset, which reflects only those portions of the original identity information needed by the services to process the requests, and a second subset, which reflects all the information in the original identity information excluding the first subset,

and the temporary assigned identity information includes ~~a~~ the first subset of original identity information for the requestors, and excludes the second subset ~~the subset reflects only those portions of the original identity information needed by the services to process the~~, the temporarily assigned identity information is monitored and removed from the protected identity directory and the local identity mapping store when terminating events are detected, and the proxy server detects and denies multiple login events that use the temporary assigned identity information ~~requests~~.

18. (Original) The identity information management system of claim 17 further comprising a local identity mapping store synchronizer that synchronizes the mappings in the local identity mapping store with one or more additional local identity mapping stores.

19. (Original) The identity information management system of claim 17 wherein the local identity mapping store, the protected identity mapping store, and the services are accessible from a secure network.

20. (Original) The identity information management system of claim 17 wherein the identity configurations are generated from one or more authoritative data stores associated with the requestors.

21. (Cancelled).

22. (Cancelled).

23. (Original) The identity information management system of claim 17, wherein the temporarily assigned identity information is randomly or deterministically generated.

24. (Original) The identity information management system of claim 17, a storage space associated with the temporarily assigned identity information is recycled or reused.

25 - 34. (Canceled).

Response to Arguments

6. Applicant's argument relative to rejection under section 101, and prior art rejection in light of the amendments noted by this action, and the telephone interview conducted on 4/7/2010 have been found persuasive (please see the attached Interview Summary).

Allowable Subject Matter

7. Amended claims 1-20, 23 and 24, now re-numbered as claims 1-22 are allowed.

Examiner's Statement of Reasons for Allowance

8. The following is an examiner's statement of reasons for allowance:

All allowed claims include a proxy server which transmits information to a service, and performs other functionalities, therefore, the proxy server is a machine or manufacture. Accordingly, all claims are directed to statutory subject matter.

All allowed claims include the features of amended independent claims 1, 10 and 17. None of the prior art of record, either taken by itself or in any combination, would have anticipated or made obvious the invention of the present application at or before the time it was filed.

Conclusion

9. Any comments considered necessary by the applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submission should be clearly labeled "comments on statement of reasons for allowance."

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Farid Homayounmehr whose telephone number is 571 272 3739. The examiner can normally be reached on 9 hrs Mon-Fri, off Monday biweekly.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edan Orgad can be reached on (571) 272-7884. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Farid Homayounmehr/
Examiner
Art Unit 2439